**Приложение № 3**

Образец

**ДО**

**„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД**

**УЛ. „ПАНАЙОТ ВОЛОВ“ № 2**

**ГР. СОФИЯ**

[наименование на участника],

представлявано от [трите имена] в качеството на [длъжност, или друго качество]

с ЕИК […], със седалище […] и адрес на управление […],

адрес за кореспонденция: […],

банкови сметки: […]

**ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ**

**за**

**участие в процедура за избор на доставчик с предмет:**

**„Закупуване на система и абонаментна поддръжка за защита от DoS/DDoS атаки за период от 3 г. за нуждите на „Информационно обслужване“ АД“**

След запознаване с документацията за участие в процедурата с настоящото техническо предложение правим следните обвързващи предложения:

1. Приемаме да изпълним доставката на системата и абонаментна ѝ поддръжка за защита от DoS/DDoS атаки за период от 3 г. за нуждите на „Информационно обслужване“ АД, съгласно всички изисквания на Възложителя, посочени в Поканата за участие и съгласно Техническото задание, в съответствие с изискванията и параметрите, посочени в тях.
2. Срок за доставка на системата и абонаментната ѝ поддръжка ……………..работни дни /*не повече от 10 (десет) работни дни*/, считано от датата на сключване на договор.
3. Техническото предложение е със срок на валидност ………….. /…………………/ календарни дни (*не по-малко от 60 календарни дни*).
4. Приемаме да осигурим възможност за обновяване по всяко време на софтуерното решение до последна версия за целия период на действие на лиценза.
5. Приемаме да доставим система и абонаментната ѝ поддръжка със следната спецификация:

|  |  |
| --- | --- |
| Спецификация на решение за DDoS защита и защита на уеб приложения | |
|  | |
| REQ. 1. | Тип решение: Хибридно решение под формата на облачна услуга и 2 бр. физически устройства за DDoS защита и защита на уеб приложения (WAF) и абонамент с включена поддръжка за период от 36 месеца. |
| REQ. 2. | Предложеното решение да включва компоненти за хибридна DDoS защита на мрежови слоеве 3 и 4, както и компоненти за Web DDoS защита и защита на уеб приложения (WAF) на мрежови слой 7. |
| REQ. 3. | Решението да включва абонамент за облачна услуга за защита. |
| REQ. 4. | Решението да включва 2 физически устройства за DDoS защита и защита на уеб приложения (WAF) и да може да се разшири с добавяне на физически устройства, които да са паралелно интегрирани с облачната услуга на същия производител, като облачната услуга за защита от производителя не може да е базирана на устройства за засичане и справяне със заплахи на други производители. |
| REQ. 5. | Решението да предоставя възможност за използване на виртуални устройства за по-малки изолирани среди или лабораторни среди. |
| REQ. 6. | Предложеното решение да е с включена платформа за управление на решението, която да може да управлява атаки с капацитет от до 40 Gbps. Лицензът за платформата за управление да включва управлението на 2 физически устройства и 10 виртуални устройства и да предоставя опция за разширяване на тези параметри в бъдеще. |
| REQ. 7. | Предложеното решение да включва 2 броя физически устройства, всяко с възможност за справяне с атаки с капацитет от до 20 Gbps. Устройствата да разполагат с по 4 слота за разширителни модули и да имат резервирано захранване (по 2 ел. захранвания на устройство) |
| REQ. 8. | Предложеното решение да включва 2 броя разширителни NIC модула (по един за всяко физическо устройство) с по 4x10G SR слотове с вътрешен байпас за всеки от модулите. |
| REQ. 9. | Предложеното решение да включва 8 броя 10GE SR (SFP+) компонента. |
| REQ. 10. | Решението да включва базов абонамент за 36 месеца за облачна DDoS защита за до 500 Mbps легитимен трафик. Абонаментът да позволява задаването на до 4 броя защитени /24 IPv4 и/или /48 IPv6 мрежови сегмента (BGP) или на до 20 защитени IP адреса (DNS). |
| REQ. 11. | Решението да включва допълнителен абонамент за периода от 36 месеца за допълнителни 50 броя защитени /24 IPv4 и/или /48 IPv6 мрежови сегмента (BGP) или на до 250 защитени IP адреса (DNS), които да се предпазват от облачната DDoS услуга с опции за използване при поискване/хибридно/винаги включена защита. |
| REQ. 12. | Решението да включва 2 броя разширителни SSL карти за физическите устройства с абонамент за 36 месеца за прилежащи функции за защита от криптирани flood атаки на база поведение, TLS инспекция, защита на приложения и информация за заплахи (threat intelligence). |
| REQ. 13. | Решението да включва базов абонамент за 36 месеца за модул за защита на облачни приложения (Облачна DDoS + WAF защита на мрежови слой 7) за 1 брой приложение и за до 50 Mbps реален HTTP/S трафик. |
| REQ. 14. | Решението да включва допълнителен абонамент за 36 месеца за защита на 5 броя допълнителни облачни приложения. |
| REQ. 15. | Решението да предоставя защита от уеб-базирани атаки срещу приложения по OWASP Top10 модела, стандартни уеб атаки, атаки с фокус върху данни и данни за достъп, както и непознати 0-day атаки. |
| REQ. 16. | Решението да включва следните функции за WAF модула: използване на негативен или позитивен модел на сигурност, защита на API, управление на ботове, контрол на достъпа, гео-политики за IP адреси, лимитиране на обема трафик към приложенията, използване на напреднали правила за сигурност, използване на ERT Active Attackers Feed (EAAF) технология за защита. |
| REQ. 17. | Решението да предоставя хибридна DDoS защита, синхронизирайки работата на облачните и на локално разположението компоненти. |
| REQ. 18. | Решението да може да инспектира криптиран (SSL) трафик. |
| REQ. 19. | Решението да предоставя функции за защита на базата на известия за случващи се в момента атаки (attackers feed), създадени и предоставени от производителя на решението. |
| REQ. 20. | Решението да разполага с автоматична синхронизация между компонентите на информация за аномално мрежово поведение и за засечени атаки (defense messaging). |
| REQ. 21. | Решението да може да синхронизира политиките за сигурност и параметрите за нормално поведение (baseline) на мрежовите процеси между локалните и облачните компоненти на решението. |
| REQ. 22. | Решението да разполага с облачна Web-DDoS услуга за справяне с атаки на мрежови слой 7 с много голям обем, като да може да засича криптирани атаки, които изглеждат като нормален трафик и използват множество техники за избягване на засичане (evasion techniques). |
| REQ. 23. | Решението да може да показва референтно сравнение на обема мрежови трафик по времето, когато няма активни атаки (в мирно време) с обема на трафика при протичаща атака, с възможност за предприемане на автоматични защитни мерки срещу атаките според обемите им. |
| REQ. 24. | Решението да може автоматично да известява при настъпила атака (като да има опция за автоматично генериране на pcap файл след завършване на атаката). Да може да се предоставя информация за параметрите на наложената политика за сигурност на решението, която е спомогнала за спирането на дадена атака. |
| REQ. 25. | Решението да може автоматично да издава различни отчети по подразбиране в различни формати по зададен график (седмични, месечни). |
| REQ. 26. | Решението да може да предоставя детайлни отчети със следствени данни (forensics) относно възникналите предишни атаки и настоящите такива. |
| REQ. 27. | Решението да може да извършва анализ на поведението на IT мрежата (network behavioral analysis). Решението да може да използва механизми за самообучение и засичане на заплахи според промените на обема мрежови трафик и други негови параметри. |
| REQ. 28. | Решението да може да засича заплахи на базата на собствена база от данни с репутации на IP адреси, която да се поддържа и обновява от производителя на решението в периода на поддръжката. |
| REQ. 29. | Решението да разполага с функции за засичане на съмнителен TCP, TLS и DNS трафик по модела challenge-response за автентикиране на източника на трафика. |
| REQ. 30. | Решението да може да предпазва от SSL Flood атаки, без да е необходимо да се предоставя ключ или сертификат на устройствата на решението. |
| REQ. 31. | Да не е необходимо да се декриптира целият мрежови трафик, за да се предпазва от SSL Flood атаки, а само трафикът от съмнителни източници, за да се намали забавянето откъм производителност на системите. |
| REQ. 32. | Решението да поддържа използването на поне 50 ръчно въведени напреднали правила за конкретни лимити (thresholds) за /32 IP съвпадения за всяка политика за сигурност на решението. |
| REQ. 33. | Решението да може да анализира поведението на DNS трафик. Да може да се изграждат сигнатури в реално време за възникнали атаки и да се автентикират източниците на мрежовия трафик за справяне с water-torture атаки, DNS flood атаки и Amplification атаки. |
| REQ. 34. | Решението да може да засича и да блокира непознати до момента заплахи (0-day защита). |
| REQ. 35. | Решението да може да засича и да блокира Web DDoS атаки чрез маркиране на криптиран HTTPS трафик като зловреден такъв на базата на познати сигнатури или на непознати пръстови отпечатъци (TLS Fingerprinting). |
| REQ. 36. | Решението да може да засича и блокира burst атаки и botnet атаки. |
| REQ. 37. | Решението да се обновява автоматично от производителя с нови сигнатури за атаки в периода на поддръжката. |
| REQ. 38. | Решението да включва услуга за техническа консултация с SOC екипа на производителя при възникване на атака, като времето за реакция от момента на известяването да е не повече от 10 минути. |
| REQ. 39. | Решението да включва предплатена услуга за имплементация и конфигурация на елементите на решението за работата на облачната DDoS защита. |
| REQ. 40. | Решението да включва предплатени професионални услуги от производителя за до 20 дни (или до 8 при физическо посещение на място) за консултации, допълнителни услуги по инсталацията на решението или провеждане на обучения на персонала на организацията. |

Прилагаме като неразделна част към настоящото предложение всички необходими документи, както следва:

*/Описват се подробно приложените документи, съгласно т. 4 от поканата, както и допълнителни документи, представени по преценка на кандидата* /

**ПОДПИС**

[качество на представляващия участника]

***Забележка:*** *Техническото предложение се представя в електронен вид във формат .pdf, подписано с квалифициран електронен подпис.*